MASSACHUSETTS DEPARTMENT OF REVENUE

TY2005

SOFTWARE DEVELOPERS USER GUIDE FOR CORPORATE, FIDUCIARY AND PARTNERSHIP E-FILE

Information Services Organization
Project Management Office
11/22/05

Currently the DOR supports one method of electronically transmitting Corporate returns in bulk. This method requires the use of an SSH client and Registration as a Professional Tax Preparer (PTP) with bulk filer option on the WebFile for Business site.

We have endeavored to make the registration and transmission process as simple as possible without compromising security. The following sections describe the registration process and the transmission process.

Registration Process

You may or may not already be registered with WebFile for Business. Choose the topic below that best matches your current registration status with the WebFile for Business site.

My Company is Already Registered as a PTP with Bulk Filer Option

All you'll need to do is update your service company information with an SSH-generated Public Key. Go to the section titled **Update My SSH-Generated Public Key.**

My Company is Already Registered as a PTP But Without Bulk Filer Option

To upgrade your status with the Bulk Filer option:

1. Login to WebFile for Business
2. Choose the "Contact DOR" link
3. On the Contact DOR form, choose the "I am a PTP and want to register for Bulk File Transfer" category, Submit the request.
4. You will receive an email when the request is approved.
5. Once you have received the approval email, log back in and proceed to update your SSH-Generated Public Key. Go to the section titled **Update My SSH-Generated Public Key** for instructions.

My Company is Registered as a Taxpayer, But Not as a PTP

You can activate your company as Professional Tax Preparer, then request bulk filer status.
To do so:

1. Login to WebFile for Business
2. From the "Account Management" menu or section page, choose the "Manage PTP Status" option.
3. Fill out the form and click the Register button. This enables your registration status immediately.
4. You must now request Bulk Filer status. Follow the steps under the section **My Company is Already Registered as a PTP But Without Bulk Filer Option**.

My Company is Not Registered With WebFile for Business

To register as a Professional Tax Preparer,

1. Point your browser at https://wfb.dor.state.ma.us/webfile/business Click the **Register** link under the "***I want to***" menu and follow the instructions for registering as a Professional Tax Preparer, and/or a Bulk File Transmitter. Make sure you select the Bulk Filer option on the registration page—otherwise you will have to make a separate request later.
2. When your registration request is approved, you will receive an email.
3. Upon receipt of your registration activation email, follow the steps under the section **Update My SSH-Generated Public Key**

Update My SSH-Generated Public Key

To update your SSH Public Key, you must be registered as a Professional Tax Preparer with Bulk Filer option, and you must have an SSH client which can generate the Public Key. If you do not have an SSH client and/or do not know how to generate the key, follow the steps under the section **Obtaining and Configuring SSH and Public Key Generation.**

Once you have your generated key, take the following steps on the WebFile for Business site:

1. Login to WebFile for Business
2. From the “Account Management” menu or section page, choose the “Manage PTP Status” option.
3. Click the Update Certificate button.
4. Paste the Public Key generated by the SSH client into the text box labeled “New Public Key Certificate” and click Set Certificate.

If your key was not in the correct format or did not update successfully, you will see an error message. Otherwise, your key has been updated. This key must be the one you use when transmitting files to the DOR via SSH.

Obtaining and Configuring SSH and Public Key Generation

File transfers to DOR are done using the SSH (Secure Shell) protocol, which provides strong encryption of network traffic. An SSH client is necessary in order to transfer your files to DOR. DOR recommends using the commercial SSH client, available from SSH Communications Security® (http://www.ssh.com/).

It's available for the Microsoft Windows® operating systems, and for several varieties of Unix, including Linux. Check the license that comes with the software for full details.

DOR may be able to assist users of the commercial SSH client with transferring files to DOR, but cannot assist users initially installing and running SSH. Support for installation and configuration should be directed to SSH customer support.

There are several freeware SSH clients, including OpenSSH, available from http://www.openssh.org, which caters mainly to Unix operating systems (although the website has links to ports to other operating systems). Although these freeware SSH clients may be successfully used to transfer files to DOR, DOR is not in a position to provide support to anyone using them.

Installing SSH

Here, we’ll only deal with the commercial SSH client under Windows. You’ll have to consult your vendor or other sources for installation of other versions of SSH and other operating systems.

As of writing, the current version of the SSH client is 4.1.1, and we’ll describe the installation and setup procedure based on that version. Other versions will probably be similar.

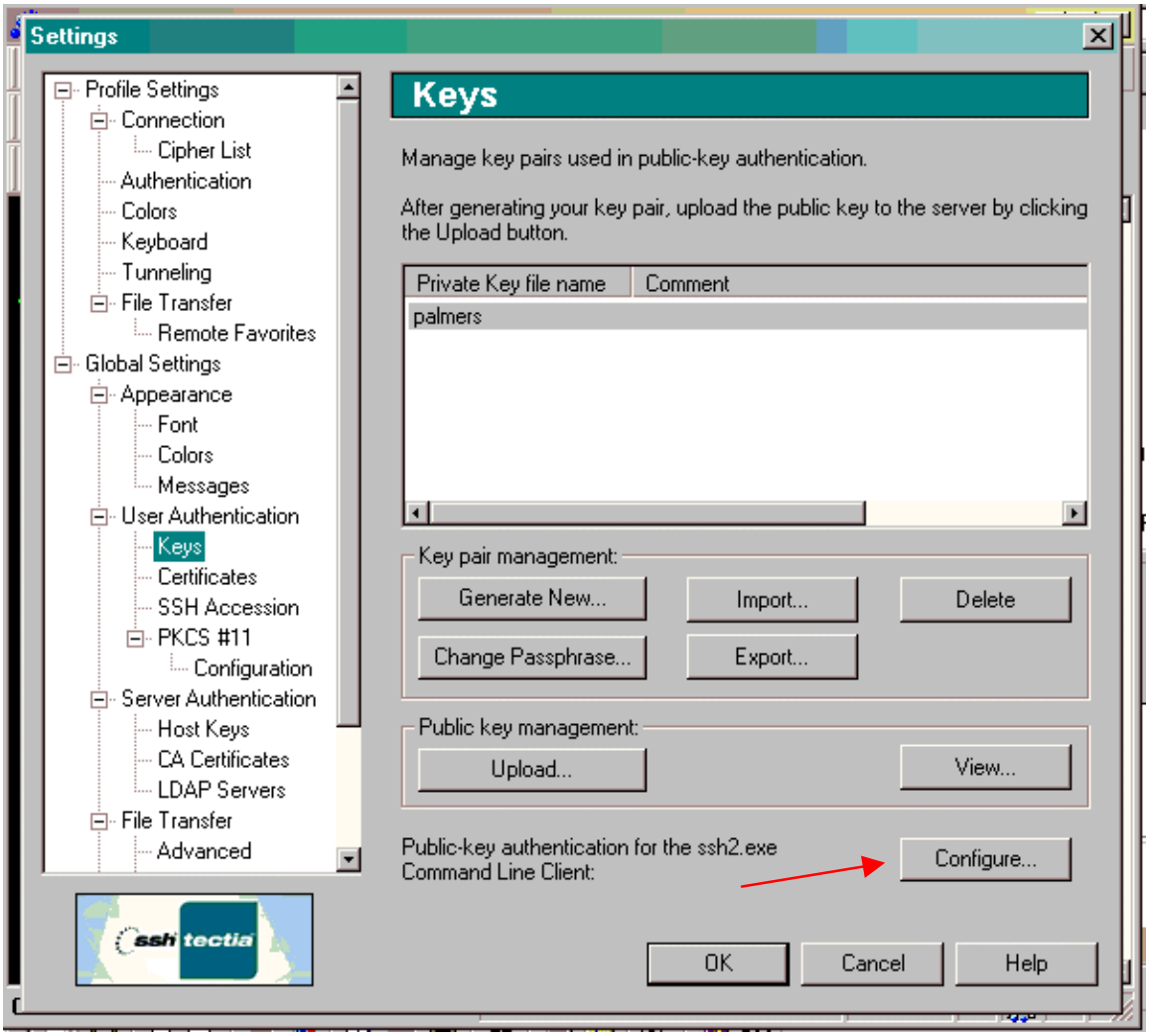
Commence installation in the usual way by double-clicking on the appropriate program and accepting any license agreements and default settings along the way. At the end of the process, you should have a desktop shortcut named “SSH Tectia Client”. Double-click on that icon, and you should be rewarded with the SSH terminal window.

Public Key Generation

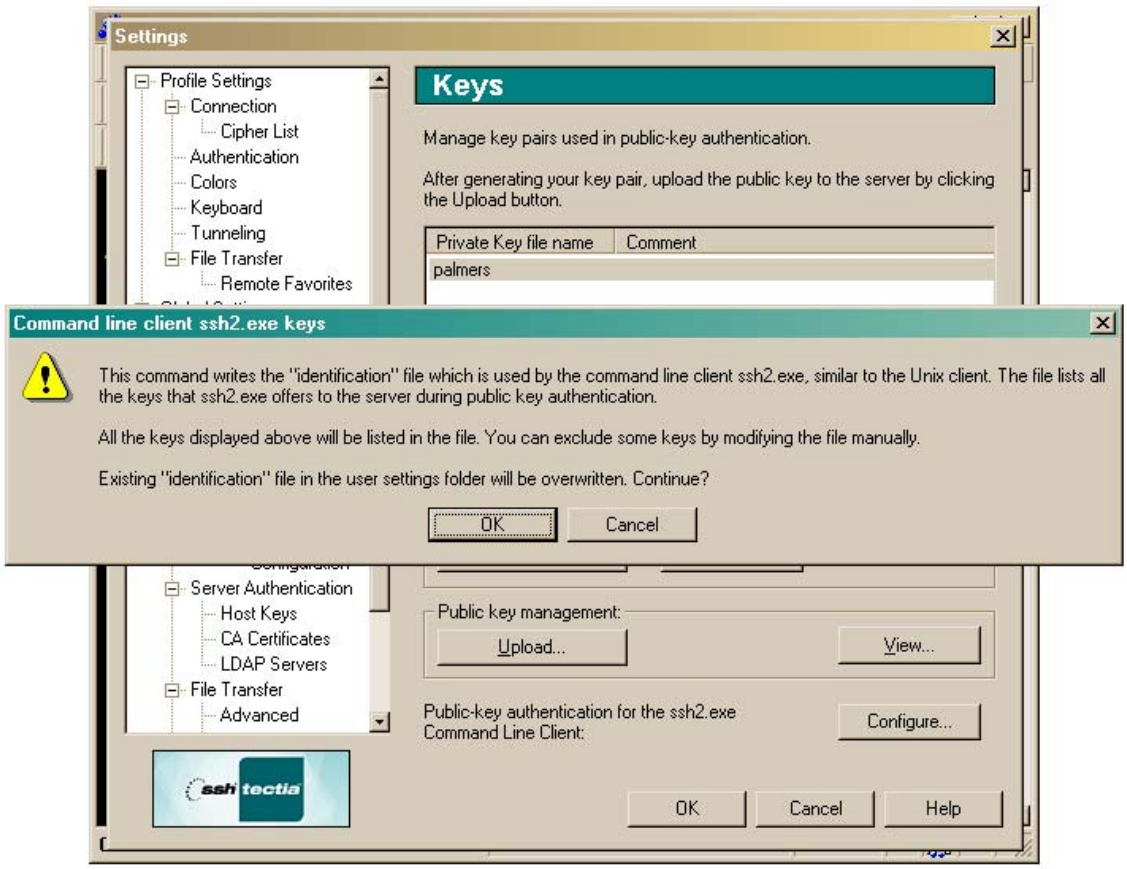
The next step is to generate your public/private key pair. The easiest way to do this with commercial SSH is to use the key-generation facilities of the GUI client:

- Under the ‘Edit’ menu, select ‘Settings…’
- Select ‘Global Settings/User Authentication/Keys
- Click on the ‘Generate New…’ button
- Follow the instructions on the dialog box, accepting default settings where applicable. The actual key generation step may take some time
- When the process completes, you are asked to click ‘Next’ to continue. Do so, and you’ll be asked for some information about your new key. Fill in the dialog as required, and click on ‘Next’.
- Click on the ‘Finish’ button. The ‘Upload Public Key’ function is of no use here.
- Click on your new key in the “Keys” window, and click on the ‘Configure’ button next to “Public key authentication for the ssh2.exe Command Line Client”. Click on ‘OK’ to overwrite and existing

identification file, Click on ‘OK’ again, and your keys should be available for use with the command-line SSH clients. The screen shot below illustrates this:

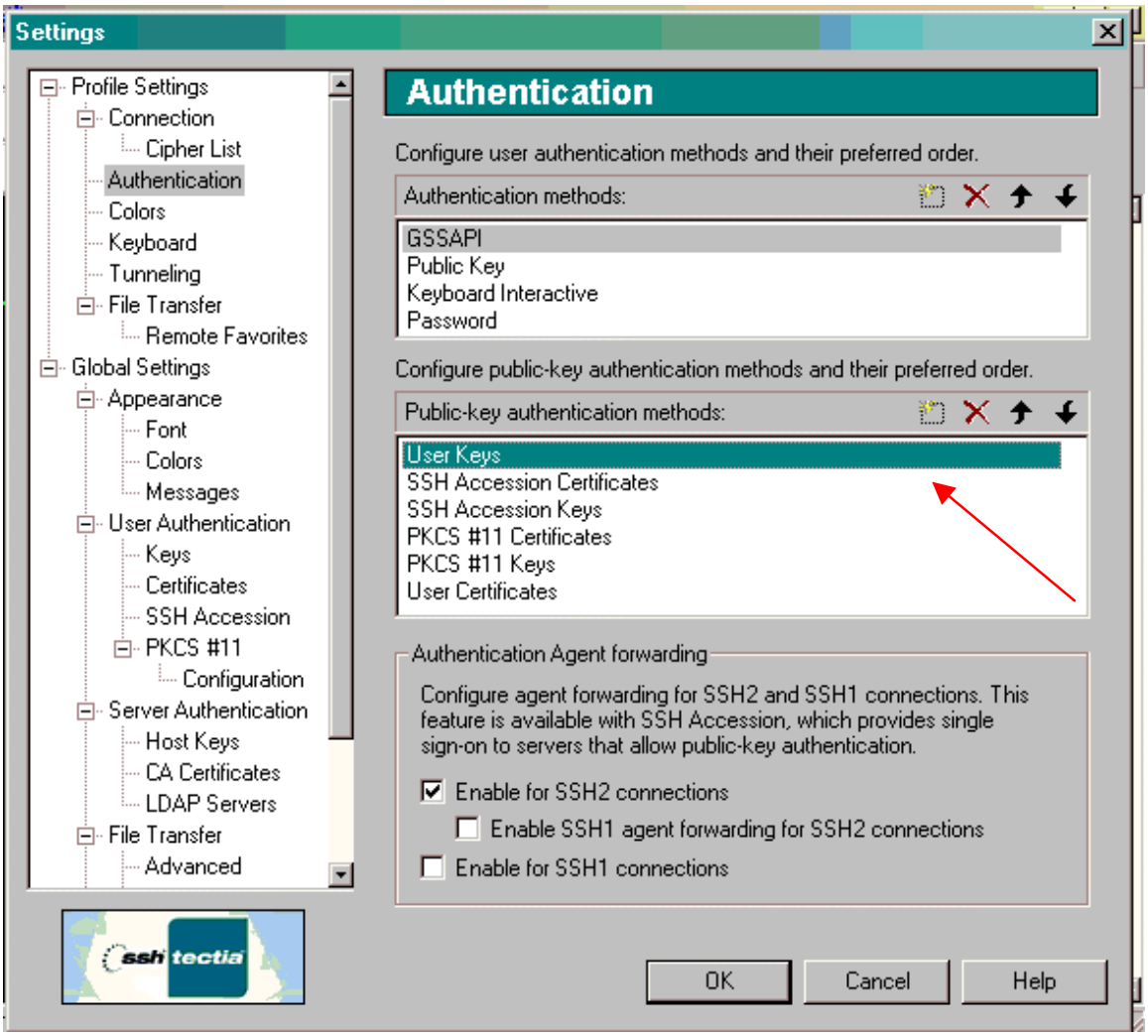


Upon clicking the Configure button, you receive a confirmation dialog similar to:



Click the OK button.

Lastly, you'll need to configure the SSH client to use User Keys. Go to Edit menu, click Settings. Under Profile Settings, click Authentication. This will bring a up a dialog where, under the section "Public Key Authentication Methods" move the line "User Keys" to the top of the list of methods if it is not already there. Click the OK button



Copying Your Public Key to the Clipboard

To copy your public key to the clipboard, ready for uploading to WebFile for Business:

- In the 'Keys' window, click on 'View…' under "Public Key Management". This will bring up a copy of Notepad with the public key in it
- Select the entire text with the mouse. Make sure you include the lines containing "BEGIN SSH2 PUBLIC KEY" and "END SSH2 PUBLIC KEY". Alternatively, hold down the control key and press the 'A' key, which should select the whole file.
- Under the 'Edit' menu, select 'Copy'

Now paste the key into WebFile for Business as detailed above.

Transmission of Files

Logging into the DOR SSH Server

Once your public key has been uploaded to DOR, you should be able to commence transferring files. Your login ID is your FID prefixed by the letters "FID". For example, if your FID is 121212121, then your SSH login ID (also known as a "username") would be: FID121212121. **Do not use your WFB login id as your SSH username. "FID" in your login should always be upper case.**

File Naming Convention

Files should be named according to their type. Extensible Markup Language files should use the extension xml. Text files (ASCII or EBCDIC) should use the extension txt. Each file name should be unique, and include the FID number used to log into the SSH server, as well as a date (4 digit year) and time (24 hour clock). Note: For batch filers, the FID numbers within wage reporting and wage withholding files are not assumed to be the same as the FID numbers used to log into SSH or as part of the filename. Beyond the FID, timestamp and extension, file names must conform to the rules required for the specific filing. Files may be sent compressed or uncompressed, compressed is preferred to conserve on network bandwidth. Compress files with any of the following: Gzip, winzip, pkzip.

Note that the term FID is synonymous with EIN.

Corporate Returns

Corporate return files have the following naming convention, **where "CORP" in the file name should always be upper case:**

Syntax:	`CORP[fid][yr][mo][day][hr][min][sec].xml`
Example:	`CORP12345678920030101145959.xml`

Where:

`[fid]`	is the FID number used to log into SSH.
`[yr]`	is the 4 digit year.
`[mo]`	is 01-12.
`[day]`	is 01-31.
`[hr]`	is 01-24.
`[min]`	is 01-60.
`[sec]`	is 01-60.

Corporate Return Acknowledgement Files

To retrieve Corporate Return Acknowledgement files, use the instructions in the section **Transfer From DOR.** The name of the acknowledgement file is the same name as the file you sent with the suffix ".ack" appended to it. Outbound files will be unzipped. So for example, if you sent the file in as named above, the acknowledgement file would be named: `CORP12121212120030101145959.xml.ack`

Initiating the Transfer (Commercial Version of SSH)

Transfers to and from DOR are performed from the command line. The GUI that comes with the commercial version is not compatible with DOR's server setup.

Transfers to DOR

If you're using the commercial SSH client, transfers to DOR can be done using either scp or sftp:

Syntax:	`scp2 [filename] [username]@[server]#[port]:upload/[filename]`
Example:	`scp2 MA941121212121200301011459 59.xml FID121212121@secure.dor.state.ma.us#444:upload/MA941121212121200301011459 59.xml`

Syntax:	`sftp2 -B [batchfile] [username]@[server]#[port]`
Example:	`sftp2 -B work.bat FID121212121@secure.dor.state.ma.us#444`

`[filename]`	Name of file to transfer.
`[username]`	FID. Example: FID`121212121`
`[server]`	DOR server = secure.dor.state.ma.us.
`[port]`	Port to connect to. DOR uses port 444.

`[batchfile]`	A file with the following FTP commands:
	`cd upload`
	`put [filename]`
	`Quit`

Transfers from DOR

These are similar to transfers to DOR, but the order of the remote and local filenames is reversed where applicable and files available for download are in a `directory` named with your user name (your `FID` name, e.g. FID`121212121`) under the general "download" `directory`.

`In addition to the direct path examples provided below, you will be able to list files by doing "ls", and to download multiple files with the "mget" command. For example, "ls download/FID121212121", and "mget download/FID121212121/*".`

`If there are no files available, the "download/username" directory` **`WILL NOT EXIST.`** `It only gets created when files are ready for download. You will need to handle this if using automated scripts.`

`Examples of direct path, single file retrieval:`

Syntax:	`scp2 [username]@[server]#[port]:download/FID121212121/[filename] [filename]`
Example:	`scp2 FID121212121@secure.dor.state.ma.us#444:download/FID121212121/MA941121212121200301011459 59.xml MA941121212121200301011459 59.xml`

Syntax:	`Sftp2 -B [batchfile] [username]@[server]#[port]`
Example:	`Sftp2 -B work.bat FID121212121@secure.dor.state.ma.us#444`

`[filename]`	Name of file to transfer.
`[username]`	FID. Example: FID`121212121`
`[server]`	DOR server = secure.dor.state.ma.us.

`[port]`	Port to connect to. DOR uses port 444.

`[batchfile]`	A file with the following FTP commands:
	`cd download\FID121212121`
	`get [filename]`
	`Quit`

Notes

The first time you connect to DOR's SSH server, you will likely be asked if you want to save the new host key. You should answer "yes" here. SSH will warn you if it detects a different host key in subsequent transfer attempts (which may mean that an unauthorized attempt is being made to eavesdrop on your communication with DOR).

DOR's public-key fingerprint is:
xinat-mopyv-veget-sesir-levib-biper-teneh-kycim-dahum-pykep-muxyx

Consult the documentation for your SSH client to determine how to use this information to confirm that the site that you've connected to is indeed DOR and has the correct public key.

Troubleshooting SSH (SCP/SFTP) connection problems

Most of the problems that filers encounter with SSH-based file transfer stem from a few common misunderstandings. Before calling the MDOR for assistance, please check the following items carefully.

Throughout this section, the words "local" and "client" refer to computers and software operated by the filer, while "remote" and "server" refer to the computers and software at the MDOR. Upper case "SSH", "SCP", and "SFTP" refer to the respective protocols, while lower-case "ssh", "scp2", and "sftp2" mean the actual programs that implement the protocols.

- All the scp2/sftp2 commands and arguments are case-sensitive. If the example says "FID", "fid" will not work. if the example says "upload", neither "UPLOAD" nor "Upload" will work.
- Be careful to distinguish the words "password" and "passphrase"; they are not the same thing. A passphrase is a secret text string that is used to protect your private key on your local client workstation; a password is used to authenticate a user at the remote server (but the MDOR SSH server does not allow users to authenticate with passwords). If you are prompted to enter a passphrase when you attempt to connect to the MDOR server, the prompt is coming from your local client software. If you are prompted for a password, the prompt is coming from the remote server. See the additional discussion at the end of this section for details.
- Make sure you are using the correct username to log in. Your SSH login username is "FIDnnn..." where "nnn..." is your 9-digit Filer ID. Your SSH username is not the username you use to log in to the WfB Website. The "FIDnnn..." username is created for you behind the scenes when you register your SSH public key.
- Make sure you are specifying destination port number 444 in your scp2 or sftp2 command. This is not the standard default port number for SSH-based connection, so your connection attempt will fail if you neglect to specify it.
- Similarly, be sure you include the remote directory specification in your commands: all uploads go to the "uploads/" directory, and all downloads are performed from the "downloads/FIDnnn..." directory. Do *not* include a slash before the directory specification. "Permission denied" errors are frequently caused by problems with directory specifications.
- If file transfers are not working, you can tell the scp2 or sftp2 program to display additional information by including a "debug" or "verbose" switch in the command, but be careful of the syntax. The scp2 program recognizes the "-v" switch, but the sftp2 program does not. Both

programs, scp2 and sftp2, recognize the "-D 2" switch. The debug switch must appear immediately after the program name (scp2 or sftp2) in the command line, before the "username@server" specification or before the "-B filename" specification. The switches are case-sensitive, lower case for "-v", upper case for "-D 2". You can use any number between 1 and 99 with the "-D" switch; higher numbers produce more detailed messages, but anything greater than 2 is likely overkill. Examples:

```
C:> scp2 -v MA941121212121200301011459 59.xml
FID121212121@secure.dor.state.ma.us#444:upload/

C:> sftp2 -D 2 -B upload.bat FID121212121@secure.dor.state.ma.us#444
```

- The command-line tools scp2 and sftp2 are independent of the GUI client, and they sometimes get confused if the GUI client is running at the same time. It is not necessary to use the GUI client to connect to the DOR. All connections and transfers can and should be performed from the command line.
- We do recommend using the GUI client for creating and managing your public key, and for configuring your SSH client software to use public-key authentication with your user key. We have found that the order in which authentication methods are specified can be important: if you are encountering authentication problems, go to the Edit menu/Settings/Profile Settings/Authentication and make sure that (1) "Public Key" is listed first in the "Authentication methods" window, and (2) "User Keys" is listed first in the "Public-key authentication methods" window.
- The server "secure.dor.state.ma.us" has two IP addresses, 4.36.198.14 and 65.202.25.14. If you are connecting through a firewall, it should permit outbound TCP connections on port 444 to both these addresses, because DNS may return either address.
- Be sure it's really an error; some messages that say "error" can be ignored, and some unexpected behaviors are correct. For example, the "upload" directory is write-only, and you will not see your uploaded file if you 'ls' the directory. This advice applies particularly to the output from the "-D" and "-v" switches.
- If you still can't find the problem, try to get a screen capture or text capture before calling the DOR. If possible, show the command you are using and the output using the "-D 2" or "-v" switch. From a Windows Command Prompt window , you can right-click on the top control bar to get a menu with an "edit/select all" option, and copy the selected text into a text file in Notepad. Or you can select the relevant section of text from the Command Prompt window with the mouse.

Additional information on passphrases and passwords:

Passphrases: When you create your public/private key pair, you will be given the opportunity to assign a passphrase to protect the private key on your local client workstation. If you choose not to assign a passphrase, your private key will be stored in a file in plaintext on your local workstation, and anyone with physical or network access to the workstation could copy the private key file and use it in combination with your public key to impersonate you. If you assign a passphrase, your private key will be encrypted in a file using the passphrase. In this case, when the client software needs to read your private key, it will prompt you to enter the key's passphrase, and it will use the passphrase to decrypt the secret key. Anyone who obtains your encrypted private-key file will find it useless without its accompanying passphrase.

The advantage to using a passphrase is, obviously, that a passphrase makes your private key more secure. There are several disadvantages, though:

1 - as with any secret word, you have to remember it. The passphrase itself is not stored in any file, database, or registry, and if you forget it, there is no way to recover it - you will have to generate a new

key pair and submit the new public key to the MDOR. If you write it down and put it in a drawer it becomes as vulnerable as any other written-down password.

2 - the rule "do not write down your passphrase" causes problems for scripting. Most filers want to automate the process of exchanging files with MDOR by writing scripts to control the scp2/sftp2 client, but there is no good way to incorporate the passphrase into a script file.

There isn't much that can be done about the first of these difficulties, but there are partial solutions for the second. Both the commercial (ssh.com) and the open-source (OpenSSH) clients provide helper applications called "SSH agents" that will hold the private-key passphrase in volatile memory and deliver it as needed to the SSH client program; these helper applications only need to be reinitialized when the local workstation is rebooted. The commercial versions of the helper programs are named ssh-agent2 and ssh-add2; the open-source versions are ssh-agent and ssh-add. The commercial SSH client can also interoperate with a separate product called Accession that manages passphrases and also supports special-purpose hardware (smartcards) for additional security; Accession, if installed, has a menu entry in the GUI client under Edit/Settings/Global Settings/User Authentication. The details of these agents are beyond the scope of this document, but information is available through the products' documentation, help systems or man pages, Web sites, and elsewhere on the Web.

Passwords: As mentioned earlier, the MDOR SSH server does not allow users to authenticate with passwords; public-key authentication is the only method that will work. Nevertheless, if your client indicates that it wants to try password authentication, the MDOR server will permit it to send a password. The order in which the different authentication methods are tried is determined by the client program. This is why we advise you to use the client GUI, Edit menu/Settings/Profile Settings/Authentication, to make sure that "Public Key" is the first item listed in the "Authentication methods" window. If you overlook this recommendation and leave "Password" listed before "Public Key", then the server will prompt your client for a password before it ever considers your public-key credentials.

This might be no more than a nuisance: if you are typing the commands yourself, you can enter any sort of junk password, allow it to be rejected, and the software will continue on to the public-key authentication step, which will presumably succeed. But if you are controlling the session with scripting you will have to write your script to detect and respond to the password prompt; this is needlessly complicated and fragile.

If you have the authentication methods listed in the order "Public Key" first, followed by "Password", then you will be prompted for a password if (and only if) your public-key authentication fails. Any password you try will be rejected, but this might be useful in some circumstances as a quick-and-dirty test to determine where a connection attempt is failing. In most cases, once testing is complete, it makes sense to specify "Public Key" as the only authentication method for SSH transfers to MDOR.

Grouping of Returns

A file may contain different types of returns. However, we request that within each file, the return types and their bottom lines be separately grouped together as follows.

First, each file should be grouped by return type: Form 355, Form 355C, Form 355S, Form 355SC, Form 2, Form 2G, Form 3.

Then, within each group of return type, we request that each be further grouped as follows:

- Group all Refund returns together
- Group all Refund returns with Overpayment carried forward together
- Group all Tax Due returns with Payments attached together
- Group all Tax Due returns without Payments together

- Group all Zero Tax Due returns together

If the transmission is not ordered this way, it will still be accepted. This will not result in an error, but your file will get processed faster if it is ordered accordingly.

Testing Criteria

In order to test your ability to send bulk returns as well as the integrity of the data of all forms and schedules, at least one file for each tax type supported must pass testing and become accepted according to the following:

At least one file for each tax type must pass testing with a minimum of five returns containing at least one instance of every form and schedule you support. If at least one return is rejected for any reason, a subsequent testing transmission is necessary containing the original testing criteia.